Fysieke Veiligheid (FV) van serverkasten is de basis

Waar moet de IT beheerder rekening meehouden

White Paper

April 2021

Door: Rashid Niamat

De vraag naar meer en betere veiligheid neemt toe. Dat heeft primair te maken met wet- en regelgeving plus het kunnen aantonen in control te zijn. Die regels overlappen deels, of zijn juist alleen geschikt voor bepaalde sectoren. Er is sprake van veel voorschriften. waarmee de inkopers, installateurs en IT beheerders rekening moeten houden. Dit whitepaper van Rittal gaat over de belangrijkste aspecten van de fysieke veiligheid van serverkasten. Die worden In de wirwar van regels te makkelijk door de IT beheerder over het hoofd gezien.

FRIEDHELM LOH GROUP

Inhoudsopgave

Introductie

Veiligheid is een breed begrip. Als het gaat om IT gaat de aandacht meer uit naar de digitale veiligheid. Op zich is dat een goede ontwikkeling. Het is immers nodig onbevoegden de toegang tot digitale data en applicaties onmogelijk te maken. De exponentiële toename van ransomware van de afgelopen periode vraagt eveneens om extra aandacht en maatregelen om IT omgevingen beter te beschermen.

De aandacht voor de data is echter niet als een scherp af te bakenen gebied te beschouwen. Data en applicaties staan op hardware. Die hardware staat weer in een serverrack. Bij de sterkere focus op de data bestaat de kans dat controle op en beheer van de serverrack met inhoud een lagere prioriteit krijgt. In dat geval is niet zeker of de beheerder in alle opzichten *in control* is.

Met dit Whitepaper vraagt Rittal aandacht voor de fysieke veiligheid van serverracks. Die beperkte scope is gekozen omdat ook op dit deelterrein al sprake is van een wirwar van regels en eisen. Doel van het document is nadrukkelijk niet alle regels en voorschriften te bespreken. Bedoeling is de lezer mee te geven dat een robuust digitale domein slechts mogelijk is als de fysieke basis aan de nodige veiligheidseisen voldoet.

EN 50600 een introductie

Voor de eerste serverrack kan worden geplaatst moet er een geschikte ruimte zijn. In het geval van nieuwbouw zal aan de hand van onder andere EN 50600 een ontwerp tot stand komen dat met tal van aspecten van de fysieke veiligheid rekening houdt.

De 10 hoofdpunten van EN 50600:

EN 50600-1:	General aspects for design and specifications
EN 50600-2-1:	Building construction
EN 50600-2-2:	Power distribution
EN 50600-2-3:	Environmental control
EN 50600-2-4:	Telecommunications cabling infrastructure
EN 50600-2-5:	Security systems
EN 50600-3-1:	Management and operational information
EN 50600-4-1:	Overview of and general requirements for key performance indicators
EN 50600-4-2:	Power Usage Effectiveness
EN 50600-4-3:	Renewable Energy Factor

EN 50600[I] is de eerste Europese norm die uitgebreide specificaties beschrijft voor de planning, bouw en exploitatie van een datacenter en daarvoor een holistische benadering hanteert.
Het definieert eisen in de criteria aspect constructie, stroomvoorziening, airconditioning, bekabeling, beveiligingssystemen en specificeert criteria voor de werking van datacenters.

De EN 50600, opgesteld door de Europese normalisatieorganisatie CENELEC (European Committee for Electro technical Standardization), biedt verschillende mogelijkheden en is daarom tot op zekere hoogte modulair opgebouwd. EN 50600 is in de eerste plaats een norm die wordt toegepast op nieuwe datacenters. Het definieert de behoefte aan deskundige adviezen en analyses tijdens het ontwerp- en constructiewerk.

Vanaf de eerste versie van En 50600 in 2012 is het framework opgebouwd rond 10 hoofdpunten. Deze zijn in dezelfde volgorde ook in de nieuwe V2.0 van voorjaar 2020 opgenomen.

Link tussen EN 50600 en ISO 27001

Dat de EN 50600 nog betrekkelijk weinig wordt genoemd in publicaties komt onder andere omdat het primair is bedoeld als een richtlijn. Daarnaast is het een puur Europese regel, met daardoor een beperkter bereik dan ISO 27001 die echt wereldwijd geldt.

De eisen en best practises die EN 50600 formuleert richten zich op de fysieke beveiliging. Daarmee is op het eerste gezicht EN 50600 strak gescheiden van ISO 27001. Die norm richt zich op het organisatorische en procesniveau om data veilig te houden.

Overigens is de strikte scheiding tussen EN 50600 en ISO 27001 er een die in de praktijk niet zo wordt ervaren. Om aan de eisen die ISO 27001 stelt te kunnen voldoen zal namelijk moeten kunnen worden aangetoond dat vanaf de constructie aan bepaalde eisen is voldaan. Er is dus sprake van een link tussen de twee. Die link is er ook tussen En 50600 en NEN 7510 die hieronder staat genoemd.

ISO 27001 en NEN 7510

Wat voor de ISO 27001 geldt speelt ook bij organisaties die naar NEN 7510 gecertificeerd zijn[II]. Die certificering die verplicht is voor elke organisatie in Nederland die toegang heeft tot medische gegevens heeft veel overeenkomsten met de ISO27001. Om die redenen zullen datacenters en ook managed providers vaak beide certificeringen hebben.

Tot de ISO 27001 en NEN 7510 eisen hoort ook dat men onderbouwd moet kunnen aantonen maatregelen getroffen te hebben om de veiligheid van de data te waarborgen. Goede fysieke beveiliging, zoals toegangsbeveiliging en bescherming tegen bedreigingen van buitenaf is belangrijk. Maar ook maatregelen tegen inbraak, stof, wateroverlast of giftige dampen moeten aanwezig zijn. Anders is men niet in control.

[I] Zie voor meer informatie over NE 50600 https://www.nen.nl/ict/datacenters/en-50600

[II] Voor meer informatie over NEN 7510 is er dit artikel
https://expert.rittal.nl/blog/nen-7510-informatiebeveiliging-gezondheidszorg/

Ook naar de maatregelen die zorgen voor een hogere mate van redundantie wordt gevraagd om antwoord te krijgen op de vraag of er voldoende maatregelen zijn getroffen om de veiligheid van de data te garanderen.

Nieuwbouw versus bestaande bouw

Voor nieuwbouw datacenters en rekencentra kan aan de hand van een bestaande EN 50600 makkelijker worden aangetoond, dat men met al die punten rekening heeft gehouden. De meeste van dit soort omgevingen in Nederland is echter niet ontworpen en (bij-) gebouwd met deze betrekkelijk nieuwe norm als leidraad.

In die gevallen is het uiteraard nog steeds mogelijk om naar ISO 27001, dan wel naar NEN 5710, gecertificeerd te worden. Het auditproces loopt dan iets anders en vergt waarschijnlijk meer tijd.

Verwarring bij verschillende klantprofielen

Van verwarring zal op dat moment nog weinig sprake zijn. Het wordt anders als het datacenter of rekencentrum verschillende klantgroepen bedient die elk een catalogus van eigen eisen en voorschriften hanteert. Gevolg zal zijn dat bij ISO 27001 voor een hele nauwe scope wordt gekozen, of dat men het zo algemeen mogelijk probeert te beschrijven.

Wat eveneens gebeurt is dat men de omgeving voor elke klantgroep afzonderlijk laat auditen, met steeds weer een andere norm als uitgangspunt. Soms is dit onvermijdelijk. NEN7510 geldt daar vaak als voorbeeld. Ruimtes die al voldoen aan ISO 27001 kunnen niet worden gebruikt voor de opslag van medische data. Daar is een extra audit voor specifiek NEN 7510 nodig. Organisaties die bepaalde financiële data verwerken of daar toegang toe hebben ontkomen niet aan een ISA3402 Type 2 en/of PCI DSS audit. Dat in dit soort gevallen sprake is van aanzienlijke kosten spreekt voor zich. Evenzo is het onvermijdelijk dat een groot aantal frameworks en richtlijnen eerder leidt tot onduidelijkheid en verwarring bij gebruikers en beheerders.

Inzoomen op fysieke veiligheid

Bovenstaande beschrijft in algemene zin de meest gebruikte normen en richtlijnen voor de bescherming van data. In veel gevallen zal daarbij sprake zijn van technische neutraal taalgebruik als het gaat om de fysieke veiligheid. “Passende maatregelen” is een omschrijving die makkelijk wordt gehanteerd.

Wat daaronder precies wordt verstaan moet keer op keer worden aangetoond aan de hand van vragenlijsten, die wel heel erg inzoomen op de details. Er moet aan veel worden gedacht. Of het nu gaat om een serverruimte met een serverrack of een compleet datacenter, de volgende punten moeten aan de orde komen.

- Hoe is de toegang tot de racks geregeld;
- Hoe is de bekabeling naar en van de racks geregeld;
- Hoe zorgt men dat de hardware in de racks onder de juiste omstandigheden kan functioneren;
- Welke procedures en maatregelen zijn er om die punten te documenteren en loggen.

Toegang tot het serverrack

Hoewel het simpele vragen lijken weet iedereen die er mee te maken heeft dat de vervolgvragen steeds complexer worden. Als men kan aantonen dat de toegang tot een serverrack is beperkt door het gebruik van sloten, is de vervolgvraag of dat ook geldt voor de ruimte waar het rack staat en of er op de kwaliteit van de sloten is gelet.

Met het beperken van de toegang tot een serverrack is een belangrijke vraag bij elke audit beantwoord. Vervolgens zal men echter moeten kunnen aantonen hoe dit wordt gecontroleerd. Om die reden is de vraag naar monitoringtools op serverrack niveau groeiende. Dit kan bestaan uit een videosysteem dat het rack of de hele ruimte bewaakt. Ook de combinatie van een cilinderslot met een persoonlijke toegangscode tot het rack of ruimte komt voor. In dat laatste geval wordt elektronisch bijgehouden op welk tijdstip een gebruiker toegang tot de rack of de serverruimte had.

Kwaliteit van het serverrack

De exacte locatie van de racks stelt eisen aan de constructie ervan. Bij datacenters zal het weinig voorkomen, maar elders moeten serverracks in vochtige of stoffige omgevingen geplaatst worden. Plaatsing in en dergelijke omgeving hoeft geen belemmering te zijn voor het in control zijn, mits men maar bekend is met de beperkingen van die locaties en daar de passende maatregelen heeft getroffen (zie ook de NEN 7510 voorwaarden). Edge computing in de procesindustrie, maar ook telecom opstellingen zijn andere voorbeelden van situaties waarin echt aandacht besteed moet worden aan het type rack.

Racks met een hoge IP waarde[III] zijn voor buitenomgevingen noodzakelijk. In bijzondere omstandigheden kan het zelfs nodig zijn het serverrack in een kluis te huisvesten.

> De **IP**-codering *(International Protection Rating, ook soms Ingress Protection)* op elektrische apparaten is een aanduiding voor de mate van beveiliging van de constructie van elektrische of elektronische apparatuur tegen eigen schade door ge-bruik in “vijandige omgevingen” en tegen eventueel gevaar voor de gebruiker. De IP-aanduiding is internationaal genormaliseerd in de norm IEC 60529. De IP-aanduiding heeft twee cijfers: het eerste geeft de beschermingsgraad tegen aanraken en indringen van voorwerpen, het tweede de beschermingsgraad tegen vocht.

Klimaatbeheersing is ook fysieke veiligheid

Als het gaat over de fysieke veiligheid van racks en de daarin aanwezige data en applicaties denkt men in de eerste plaats aan de toegang tot de hardware. Dat de stroomvoorziening en connectiviteit bescherming nodig heeft is eveneens duidelijk. Klimaatbeheersing staat echter minder vaak op het netvlies.

Toch is klimaatbeheersing een uiterst belangrijke factor bij het beschermen van zowel data als hardware. Binnen EN 50600 2-3 wordt klimaatbeheersing beschreven. Het heeft geen directe link met ISO 27001 of NEN 7510. Veel meer is het dat bij vragen over de robuustheid en redundantie van de gekozen oplossingen aangetoond moet worden dat er passende maatregelen zijn getroffen.

[III] Definitie is afkomstig van https://nl.wikipedia.org/wiki/IP-code

Daarbij wordt naar het geheel van HVAC maatregelen gekeken. Voor de bepaling of er sprake is van afdoende maatregelen om business continuïteit te waarborgen wordt HVAC tegenwoordig standaard onder de loep genomen. Mede om die reden kiest men bij kleinere installaties vaker voor serverracks waarin af fabriek HVAC zijn geïntegreerd.

Dan is er nog de AVG

Technisch gezien zijn er amper belemmeringen om tot het juiste niveau van fysieke veiligheid te komen. Ruimtes die gecertificeerd moeten worden ontkomen er ook niet aan daar keuzes te maken.

Daarmee is echter niet gezegd dat het overal hoog genoeg op de agenda staat. Of het nu gaat om nieuwbouw of uitbreidingen van serverruimtes, de kans is aanwezig dat men aan de fysieke veiligheid minder aandacht besteedt. Het speelt vooral bij de kleinere organisaties. Stilstaan bij fysieke veiligheid gebeurt ook te weinig bij bedrijven die over de jaren meer met persoonsgegevens zijn gaan doen – en dat is een hele grote groep.

Voor al die bedrijven geldt dat ze echt veel meer met regelgeving te maken hebben die impliciet dwingt na te denken over de fysieke veiligheid. Sinds 2016 er de AVG[iv], die voorschrijft dat iedereen moet kunnen aantonen 'passende maatregelen te hebben getroffen" of het verlies en misbruik van persoonsgegevens tegen te gaan. Het gaat daarbij om gegevens van klanten, leveranciers en ook het eigen personeel.

Alleen al daardoor heeft iedere ondernemer met de AVG te maken. Voor veel ondernemers is IT een hulpmiddel om de activiteiten te kunnen uitvoeren. Nadenken over het beschermen van de IT is nieuw. De eisen die de AVG stelt komen daarbij als breed en vaag over. Dat wekt verwarring in de hand, helemaal als het gaat om het invullen van het begrip "passende maatregelen".

Inmiddels groeit wel het besef dat aandacht besteedt moet worden aan de fysieke veiligheid van de hele werkomgeving, inclusief de hardware en serverracks. Het is namelijk de onmisbare basis om tot goede bescherming van persoonsgegevens te komen.

In artikel 32 van de AVG (voluit de Algemene Verordening Gegevensbescherming) staat dat bedrijven en overheden passende technische en organisatorische maatregelen moeten nemen om de veilige verwerking van persoonsgegevens mogelijk te maken. De Autoriteit Persoonsgegevens heeft daarover de volgende toelichting:

- *Organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen.*
- *Verder moeten ze niet alleen naar de techniek kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?*

Via dit artikel worden door de AVG dus eisen gesteld aan de fysieke veiligheid van IT omgevingen waar persoonsgegevens opgeslagen zijn.

[iv] De integrale tekst van deze Verordening staat op de website van de toezichthouder https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Rittal B.V.
Hengelder 56 · Postbus 246 · 6900 AE ZEVENAAR
Tel.: (0316) 59 16 60 · Fax: (0316) 52 51 45
E-mail: sales@rittal.nl · www.rittal.nl

Voor meer informatie met betrekking tot dit onderwerp:
Edgar Hoogakker · Product Manager Klimatisering · E-mail: ehoogakker@rittal.nl